

AUG 1983

STAT

NSA review completed

NATIONAL SECURITY DECISION
DIRECTIVE NO. _____

NATIONAL POLICY ON TELECOMMUNICATIONS/AUTOMATED
INFORMATION SYSTEMS SECURITY

It is the responsibility of the Executive Branch to properly safeguard information which concerns the security and other vital interests of the United States, including government-held information which bears on the individual rights or privacy of U.S. persons. Telecommunications and other information systems which handle such information in electronic form are inherently vulnerable to interception, unauthorized electronic access, and related means of technical exploitation. Assuring their security integrity is therefore a national responsibility.

1. Objectives. To fulfill these responsibilities, I direct that the nation's capabilities for securing telecommunication and automated information systems against technical exploitation threats be developed, improved, and maintained as necessary to:
 - a. Assure availability of an adequate technical base within both government and industry.
 - b. Provide for reliable and continuing assessment of threats and vulnerabilities.
 - c. Support other existing policy objectives for national telecommunications and automated information resources.
 - d. Ensure effective use of protection resources.

2. Policy Elements. National policy for the protection of telecommunications and automated information systems shall encompass the following elements:

a. Systems which generate, store, process or transmit classified information in electrical form shall be secured against exploitation.

b. Systems similarly handling other government-derived information, the loss of which could adversely affect the national interest or the rights of U.S. persons, shall be protected commensurate with the risk of exploitation.

c. Systems which handle non-government information of similar nature should be protected commensurate with the threat of exploitation. The Government shall take necessary steps to identify such systems and information and formulate strategies and measures for providing protection. The private sector shall be encouraged to undertake the application of such measures in the national interest.

3. Implementation.

a. A Systems Security Steering Group is hereby established to ensure a coordinated and effective national effort, and shall consist of the following:

(1) The Assistant to the President for National Security Affairs, or his representative. (Chairman)

(2) The Executive Agent for Communications Security/Executive Agent of the National Communications Systems (NCS).

(3) The Director of Central Intelligence.

(4) The Associate Director of the Office of Management and Budget (OMB) for National Security and International Affairs.

(5) The Director, National Security Agency (NSA). (Executive Secretary).

b. The Steering Group shall:

(1) Oversee the implementation of and provide guidance to the National Information Systems Security ^{Committee} ~~Group~~ with respect to the objectives and policy elements stated herein.

(2) Establish broad national objectives and priorities as may be required to implement this Directive.

(3) Review and approve consolidated resources program and budget proposals, and other matters referred to it by the Executive Agent in fulfillment of responsibilities outlined in subparagraph (4), below.

(4) Annually review and evaluate the security status of national telecommunications and automated information systems ^{submitted by government agencies} with respect to established objectives and priorities. ^{of the Directive}

(5) Interact with the Steering Group on National Security Telecommunications[?] and, through that Group, with the National Security Telecommunications Advisory Committee (NSTAC), to ensure that the objectives and policy elements of this Directive are addressed.

(6) Recommend for Presidential approval additions or revisions to this Directive as national interests require.

4. The National Information Systems Security Committee.

a. The National Information Systems Security Committee (NISSC) is hereby established and will operate under the direction of the Systems Security Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be composed of a representative of each of the following:

The Secretary of State
The Secretary of The Treasury
The Secretary of Energy
The Secretary of Transportation
The Attorney General
The Secretary of Commerce
The Director, Office of Management and Budget
The Chief of Staff, United States Army
The Chief of Naval Operations
The Chief of Staff, United States Air Force
The Chairman, Joint Chiefs of Staff
The Director, Central Intelligence Agency
The Director, Federal Emergency Management Agency

*
representation

The Administrator, General Services
Administration

The Manager, National Communications
System

The Director, National Security Agency
(voting Chairman)

b. The Committee shall:

(1) Establish such specific operating policies, objectives, and priorities as may be required to implement this Directive.

(2) Submit to the Systems Security Steering Group an annual evaluation of the status of national telecommunications and information resources security with respect to established objectives and priorities.

(3) Administer matters pertaining to the release of sensitive security information, techniques, and materials to foreign governments or international organizations, *except in intelligence operations managed by the Dir CIA.*

(4) Establish and maintain a national issuance system for promulgating the operating policies, directives and guidance which may be issued pursuant to this Directive.

(5) Establish ~~permanent and temporary~~ *chaired by the DCI for sensitive intelligence operations. Its membership shall be composed of* subcommittees as necessary to discharge its responsibilities. *members nominated by*

(6) Other subcommittees shall be established as necessary.
e. The Committee shall make recommendations to the *the DCI*

Steering Group on Committee membership, and may establish criteria and procedures for permanent observers.

Representatives of other departments or agencies affected by specific matters under deliberation will attend upon invitation of the ~~Chairman~~ *Steering Group*.

f. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency. The secretariat may be augmented as necessary by personnel provided by the Departments and Agencies represented on the Board in response to the Chairman's request. The National Security Agency shall provide facilities and support as required.

3. The Executive Agent of the Government for Communications Security.

The Secretary of Defense is the Executive Agent of the Government for Communications Security. In this capacity he shall serve an expanded role to act within policies and procedures established by the Systems Security Steering Group and the NISSC to:

a. Ensure the development, in conjunction with NISSC member Departments and Agencies, of plans to fulfill the objectives of this Directive, including the formulation of necessary security architectures.

b. Fulfill requirements of the Federal Government for ^{*Communications*} ~~technical~~ security material and related services.

c. Provide or approve ^{*minimum*} security standards and doctrine.

DRAFT

d. Conduct or approve research and development of security techniques and equipment.

e. Operate or coordinate the efforts of Government technical centers related to telecommunications and automated information systems security.

f. Develop and submit to the Steering Group and the Congress a proposed National Telecommunications and Information Systems Security Program budget for each fiscal year.

6. The Director, National Security Agency.

The Director, National Security Agency is responsible for ~~executing~~ *managing - acting as executive agent* the foregoing responsibilities of the

Secretary of Defense as Executive Agent. In fulfilling these responsibilities he shall have authority to:

a. Empirically examine federal telecommunications and associated electronic information handling systems *except specific intelligence community (I.C.) functions additional by the DCI* and evaluate their vulnerability to hostile *(see para 11)* interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with the law and other applicable directives. *the DCI shall be responsible for examining and reporting the status of specific exempt I.C. activities.*

b. Act as the single government focal point for all matters related to cryptography to include; conducting research and development; prescribing or approving all standards, techniques, systems and equipments; and conducting

DRAFT

liaison with foreign governments, international organizations, and private institutions *(I.C. operations to be coordinated with DCI)*

c. Operate such industrial facilities as may be required to perform critical functions related to the provision of cryptographic and other sensitive security materials or services.

d. Operate a central technical center(s) to assess and disseminate information on hostile threats to national telecommunications and information systems security *responsible government agencies as appropriate,*

e. Operate a central technical center(s) to *perform* evaluate the security of telecommunications systems, computer systems and data networks, and to conduct or sponsor research and development of security techniques.

f. Prescribe the *minimum acceptable* control systems and standards for protecting cryptographic and other sensitive security material, techniques, and information.

7. The Director of Central Intelligence shall, *as he deems necessary,* identify to the NISSC and the Director, NSA, as appropriate, any unique handling requirements associated with the protection of sensitive compartmented intelligence.

8. The Secretary of Commerce, through the Director, *of the* National Bureau of Standards, shall issue such standards for the security of telecommunications and other electronic information resources as the *NISSC* Director, NSA may approve and authorize for public release in accordance with authorities assigned herein.

9. The Director, Office of Management and Budget shall review for consistency with this Directive, and amend as appropriate, OMB Circulars A-71 (Transmittal Memorandum No. 1), OMB Circular A-76 as amended, and other OMB policies and regulations which may pertain to the subject matter herein.

10. The Heads of Federal Departments and Agencies shall:

a. Conform with any policies, standards and doctrines issued by proper authority pursuant to this Directive.

b. Provide to the Systems Security Steering Group, the NISSC, the Secretary of Defense as Executive Agent, and the Director, National Security Agency such information as they may require to discharge responsibilities assigned herein.

11. Nothing in this Directive shall:

a. Alter the existing authorities of the Director of Central Intelligence for the overall ^{directing, management,} ~~direction~~, coordination and supervision of intelligence matters, nor his responsibility to act as Executive Agent of the Government for technical security countermeasures (TSCM) against bugging, eavesdropping and related forms of surveillance ^{or attempts to procure} ~~national security information handled in any COMSEC system.~~

b. Give ~~the~~ the NISSC, the Secretary of Defense, or the Director, National Security Agency authority to inspect the personnel, facilities, or internal operations of other departments and agencies without their approval. This provision does not constrain the authority of the Director, NSA to monitor

telecommunications or the emissions of other electronic information systems consistent with paragraph 11.a., above.

c. Amend or contravene the provisions of other, existing directives which may pertain to the financial management of automated information resources or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

12. For the purposes of this Directive, the following terms shall have the meanings indicated.

a. Telecommunications means the creation, preparation, manipulation, transmission, communication or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

b. Automated Information Systems means systems which create, prepare, manipulate or process information in electronic form for purposes other than telecommunication, and includes computers, word processing systems and associated equipment.

c. Telecommunications and Information Systems Security means protection afforded to telecommunications, automated information systems, and other electronic information handling systems in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security,

emission security, and computer security) to systems which generate, handle, or process information of use to an adversary, and also includes physical protection of sensitive security resources and materials.

13.. PD/NSC-24 is hereby superseded.

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Position Paper of the Office of Security on the Proposed PD/24

FROM:

NO.

DATE

8 SEP 1983

TO: (Officer designation, room number, and building)

DATE

OFFICER'S INITIALS

RECEIVED

FORWARDED

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

1. DD/P&M
4E63 Hqs

2.

3. DD/Sec
4E63 Hqs

4.

5. D/Sec
4E63 Hqs

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

THE DAVIS STUDY IS UNDER
SOURCES AND METHODS TYPE
PROTECTION IS AT THE REAL
ROOT OF FOUR CENTERS
WE HAVE UNIQUE PROBLEMS
IN CIA!

9/8/83